Deutscher Bundestag **Drucksache 16/4997**
16. Wahlperiode 10. 04. 2007

Antwort
der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Gisela Piltz, Sabine Leutheusser-Schnarrenberger, Jörg van Essen, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 16/4795 –

Online-Durchsuchungen

Vorbemerkung der Fragesteller

Im Rahmen der Feststellung des Haushaltsplanes für das Haushaltsjahr 2007 wurde im Geschäftsbereich des Bundesministeriums des Innern das Programm zur Stärkung der Inneren Sicherheit (PSIS) mit der Mehrheit der Regierungskoalition von CDU, CSU und SPD beschlossen. Im Rahmen dieses Programms wurden Mittel vorgesehen, um Möglichkeiten zu entwickeln, „entfernte PCs" auf „verfahrensrelevante Inhalte hin" zu durchsuchen, „ohne tatsächlich am Standort des Geräts anwesend zu sein".

Diese Vorgehensweise wurde als „Online-Durchsuchung" bekannt. Der Bundesgerichtshof hat mit Beschluss vom 25. November 2006 festgestellt, dass für ein derartiges Vorgehen keine Rechtsgrundlage besteht.

Der Bundesminister des Innern, Dr. Wolfgang Schäuble, kündigte daraufhin in einer Pressemitteilung am 5. Februar 2007 an, nun eine Rechtsgrundlage für die Online-Durchsuchungen schaffen zu wollen. In einem Interview mit dem „Kölner Stadt-Anzeiger" vom 8. Februar 2007, welches auch auf der Homepage des Bundesministeriums des Innern eingestellt ist, spricht er sich zudem dafür aus, die Online-Durchsuchungen sowohl der Polizei als auch dem Verfassungsschutz zu ermöglichen.

1. Werden die im PSIS vorgesehenen Forschungen und Entwicklungen zur Online-Durchsuchung aktuell weiterverfolgt?

Das Bundeskriminalamt (BKA) hat nach § 2 Abs. 6 Nr. 3 des Bundeskriminalamtsgesetzes als Zentralstelle zur Unterstützung der Polizeien des Bundes und der Länder polizeiliche Methoden und Arbeitsweisen der Kriminalitätsbekämpfung zu erforschen und zu entwickeln. Dies setzt voraus, dass das BKA auch neue technische Verfahren im Hinblick auf ihre Eignung als Ermittlungsinstrumente der Strafverfolgung prüft und bewertet, auch unabhängig davon, ob eine Durchführung entsprechender Maßnahmen unmittelbar bevorsteht oder entsprechende Rechtsgrundlagen bereits zur Verfügung stehen. Was die Frage von Online-Durchsuchungen angeht, wird im BKA derzeit die technische Umsetz-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 5. April 2007 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

barkeit einer solchen Maßnahme im Rahmen eines Entwicklungsprojektes geprüft. Dies ist noch nicht abgeschlossen.

2. Wenn nein, was geschieht mit den dafür vorgesehenen Mitteln, und wird der Plan, Online-Durchsuchungen zu erreichen, vollständig aufgegeben, bzw. wie soll dieser Plan unter der aktuellen Rechtslage weiterverfolgt werden?

Auf die Beantwortung zu Frage 1 wird verwiesen.

3. Welche Planungen bestehen innerhalb des Bundesministeriums des Innern und innerhalb der Bundesregierung zur Schaffung einer Rechtsgrundlage für Online-Durchsuchungen?

Die Frage, in welchen Gesetzen des Bundes eine Rechtsgrundlage für eine Online-Durchsuchung erforderlich ist, wird derzeit innerhalb der Bundesregierung geprüft. Diese Prüfung ist noch nicht abgeschlossen.

4. Welche technische Lösung wird bzw. wurde bei der Online-Durchsuchung verfolgt?

   Werden sich selbst installierende Programme entwickelt, um so genannte Schadsoftware bzw. Trojaner – in den Medien „Bundestrojaner" genannt – in PCs einzuschleusen, und/oder werden Absprachen mit den Softwareherstellern angestrebt mit dem Ziel, dass diese gezielt Sicherheitslücken in ihrer Softwarearchitektur offenlassen, um den Ermittlungsbehörden den Zugriff auf die im Internet angeschlossenen PCs zu ermöglichen?

   Welche Vor- und Nachteile sieht die Bundesregierung in den verschiedenen Möglichkeiten?

Im BKA wird derzeit die technische Umsetzbarkeit einer Online-Durchsuchung im Rahmen eines Entwicklungsprojektes geprüft. In welcher Ausgestaltung diese Maßnahme als polizeiliches Mittel tauglich ist, kann erst nach weiterer Entwicklung bewertet werden. Bei der Entwicklung werden besonders die Aspekte der Gerichtsverwertbarkeit der Ergebnisse, der Nichtweiterverbreitung von hierzu verwendeten Programmen und des weitestgehenden Ausschlusses unerwünschter Effekte berücksichtigt. Konkrete Aussagen lassen sich hierzu jedoch noch nicht treffen. Absprachen mit Herstellern von Software werden dabei nicht angestrebt.

Über geheimhaltungsbedürftige Einzelheiten der Tätigkeit des Bundesnachrichtendienstes, des Bundesamtes für Verfassungsschutz und des Militärischen Abschirmdienstes können Auskünfte der Bundesregierung nur gegenüber den zuständigen parlamentarischen Kontrollgremien erfolgen.

5. Wenn Sicherheitslücken in der Software für Online-Durchsuchungen genutzt werden sollen/sollten, wie will/wollte die Bundesregierung dem Problem begegnen, dass auch Kriminelle sich diese Lücken zunutze machen könnte und wie will/wollte die Bundesregierung dem Problem begegnen, dass Software international identisch ist und daher eine international einheitliche Sicherheitslücke angestrebt und mit allen anderen betroffenen Staaten abgesprochen werden müsste und daher auch fremde Geheimdienste und ggf. andere fremde Behörden Zugriff auf die in Deutschland befindliche an das Internet angeschlossenen PCs erhielten, und wie soll verhindert werden, dass beispielsweise auch eine von deutschen Behörden kryptografisch abgesicherte Software zur heimlichen Online-Durchsuchung von PCs Kriminellen, Terroristen und gegnerischen Geheimdiensten in die Hände fällt?

Die Schaffung von Sicherheitslücken wird nicht angestrebt. Derzeit wird davon ausgegangen, dass durch technische Maßnahmen weitestgehend verhindert wer-

den kann, dass die einzusetzenden Programme von unbefugten Dritten für eigene Zwecke missbräuchlich benutzt werden. Abgesehen davon, dass ein Entdeckungsrisiko eines solchen Programms gering einzustufen ist, wäre eine Manipulation dieses Programms im Vergleich zu anderen über den Markt bereits bestehenden Möglichkeiten extrem aufwändig. Im Übrigen wird auf die Beantwortung zu Frage 4 verwiesen.

6. Wenn „Trojaner“ genutzt werden sollen/sollten, auf welchem Weg sollen/sollten diese auf den zu durchsuchenden Festplatten installiert werden: durch täuschungsbedingte Selbstinstallation durch den Benutzer der Festplatte und/oder soll physisch in die Räumlichkeiten bis zum PC vorgedrungen werden, um eine solche Software aufzuspielen, oder auf welche andere Weise?

Auf die Beantwortung zu Frage 4 wird verwiesen.

7. Wenn „Trojaner“ genutzt werden sollen/sollten, wie soll/sollte dem Problem begegnet werden, dass Kriminelle einen erkannten „Bundestrojaner“ kopieren und benutzen, und wie soll/sollte dem Problem begegnet werden, dass die Softwareindustrie Antivirenprogramme und „Firewalls“ auf die Bedrohung durch diese „Trojaner“ hin entwickelt bzw. verbessert?

Auf die Beantwortung zu Frage 5 wird verwiesen.

8. Sieht die Bundesregierung die Gefahr eines digitalen Wettrüstens, wenn Kriminelle einen „Bundestrojaner“ oder eine bewusste Sicherheitslücke in der Software entdecken und die Software daraufhin angepasst werden muss und neue „Bundestrojaner“ bzw. Sicherheitslücken geschaffen werden müssen, welche wiederum von Kriminellen entdeckt werden usw., und wie schätzt die Bundesregierung die Folgekosten eines solchen Wettrüstens ein?

Eine solche Gefahr wird nicht gesehen. Das Ergreifen möglicher Gegenmaßnahmen durch die Zielperson und eine Reaktion der Ermittlungsbehörden hierauf ist keine Besonderheit der Online-Durchsuchung, sondern tägliche Praxis. Im Übrigen wird auf die Beantwortung zu Frage 5 wird verwiesen.

9. Hält es die Bundesregierung für vereinbar, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) auf der einen Seite die Aufgabe der technischen Prüfung der technologischen Sicherheit und Zuverlässigkeit und auf der anderen Seite die Aufgabe der Entwicklung von technischen Möglichkeiten zur Überwindung der technischen Sicherheitsarchitektur in der Informationstechnologie zuzuweisen?

   Inwieweit sieht die Bundesregierung eine Gefahr, das Vertrauen in das BSI durch die Übertragung der Aufgabe der Entwicklung von technischen Möglichkeiten zur Online-Durchsuchung zu beschädigen?

Aufgabe des Bundesamtes für Sicherheit (BSI) in der Informationstechnik ist es, die Sicherheit der Informationstechnik zu fördern. Diese präventive Funktion wird durch IT-Sicherheitsuntersuchungen, IT-Sicherheitsempfehlungen sowie die Beratung und Unterstützung von Behörden, Unternehmen und Bürgerinnen und Bürgern wahrgenommen. Das BSI ist nicht beauftragt, technische Möglichkeiten zur Durchführung von Online-Durchsuchungen zu entwickeln. Eine Gefahr, das Vertrauen in das BSI zu beschädigen, sieht die Bundesregierung daher nicht.

10. Wie weit sind die Möglichkeiten der Ermittlungsbehörden des Bundes nach dem aktuellen technischen und wissenschaftlichen Stand der Computerforensik und auch im Hinblick auf den Ausbildungsstand der Mitarbeiter gegeben, auch gelöschte Daten auf Festplatten und die letzten Internetverbindungsdaten, welche sich auf der Festplatte befanden, wiederherzustellen?

Die auf dem Gebiet der Computerforensik eingesetzten Mitarbeiter des Bundes verfügen über ein dem aktuellen Stand der Wissenschaft und Technik entsprechendes Wissen und entsprechende technische Ausstattung. Die Wiederherstellung nicht endgültig gelöschter Daten ist grundsätzlich möglich. Internet-Verbindungsdaten, im Sprachgebrauch des Telekommunikationsgesetzes Verkehrsdaten, werden grundsätzlich nicht beim Nutzer, sondern durch den jeweiligen Telekommunikationsdiensteanbieter erhoben und gegebenenfalls gespeichert.

11. Wie schätzt die Bundesregierung das Entwicklungspotential der Computerforensik in dieser Hinsicht ein?

Das Problem der endgültigen Löschung von Daten auf Datenträgern bleibt bestehen.

12. Wo liegen nach Ansicht der Bundesregierung die Erkenntnis- und Beweisvorteile einer Online-Durchsuchung auf der einen Seite gegenüber einer Präsenzdurchsuchung mit Beschlagnahme der entsprechenden Datenträger und der Überwachung der elektronischen Post im Rahmen der Telekommunikationsüberwachung auf der anderen Seite?

Die Bundesregierung prüft derzeit die technischen Möglichkeiten und die rechtlichen Voraussetzungen so genannter Online-Durchsuchungen. Die Frage wird sich erst nach Abschluss dieser Prüfung beantworten lassen.

13. Inwieweit können anhand der absehbaren Fortschritte in der Computerforensik in Zukunft im Nachgang einer Beschlagnahme von Datenträgern nach Einschätzung der Bundesregierung dieselben Daten beweisfähig gesichert werden, welche nach heutigem Erkenntnisstand nur bei einer Online-Durchsuchung beweissicher erlangt werden können?

Flüchtige, das heißt nur im Arbeitsspeicher des Rechners befindliche, und endgültig gelöschte Dateien können im Nachgang einer Beschlagnahme von Datenträgern nicht erlangt werden; ebenso ist der Zugriff auf verschlüsselte Inhalte deutlich erschwert oder gar unmöglich.

14. Inwieweit handelt es sich nach Ansicht der Bundesregierung in dem Fall, dass über die Online-Durchsuchung mittels Auffinden entsprechender „Cookies“ oder auf andere Weise herausgefunden werden soll, ob jemand inkriminierte Online-Kommunikation getätigt hat oder ob anderweitige inkriminierte Daten auf der Festplatte vorhanden sind, von einer herkömmlichen Durchsuchung mit Beschlagnahme der Festplatte aber wegen dem warnenden Effekt bzw. der für einen Durchsuchungsbeschluss nicht ausreichenden Beweislage abgesehen wird, um Ermittlungen ohne konkreten Anfangsverdacht?

Nach dem deutschen Strafprozessrecht dürfen repressive Ermittlungsmaßnahmen nur im Rahmen eines Ermittlungs- bzw. Strafverfahrens durchgeführt werden. Die Einleitung eines solchen Verfahrens setzt nach § 152 der Strafprozess-

ordnung voraus, dass zureichende tatsächliche Anhaltspunkte für eine verfolgbare Straftat vorliegen. Liegt ein solcher Anfangsverdacht nicht vor, sind sowohl offene als auch verdeckte strafprozessuale Ermittlungsmaßnahmen unzulässig.

15. Sind diese Ermittlungen aus Sicht der Bundesregierung gerechtfertigt und/oder wünschenswert, und welche Anlassschwelle muss nach Ansicht der Bundesregierung für eine Online-Durchsuchung überschritten sein?

Für eine „verdachtslose“ Online-Durchsuchung – etwa in Gestalt einer umfassenden Rasterung von Internetcomputern zum Zwecke der Verdachtsschöpfung – besteht aus strafverfahrensrechtlicher Sicht kein rechtfertigender Anlass.

16. Wenn der Online-Zugriff auf die Festplatte erfolgreich ist, wie sollen/sollten die gesuchten Daten auf der Festplatte aufgefunden werden, und wie soll/sollte vermieden werden, dass dabei auch Daten aus dem geschützten höchstpersönlichen Lebensbereich des Benutzers der Festplatte erfasst werden?

Auf die Antwort zu Frage 12 wird verwiesen.

17. Soweit bei der Erfassung der Daten während einer Online-Durchsuchung mit Schlagwörtern gearbeitet werden soll/sollte, wie soll/sollte dem Problem begegnet werden, dass nur Menschen, nicht aber Software eine „moralische“ – bzw. eine die rechtlich zutreffende Abwägung widerspiegelnde – Auswahl hinsichtlich der gesuchten und der – weil dem geschützten höchstpersönlichen Lebensbereich zugehörig – nicht zu erfassenden Daten treffen können?

Die Suche würde sich aufgrund der jeweiligen Anordnung auf Daten beschränken, die für das zu Grunde liegende Ermittlungsverfahren von Bedeutung sind. Eine eventuelle technische Vorauswahl würde lediglich als Hilfsmittel dienen und einer herkömmlichen Durchsuchung entsprechen, bei der Papiere zunächst nur grob auf eventuelle Relevanz geprüft werden. Im Übrigen wird auf die Beantwortung zu Frage 4 verwiesen.

18. Soweit nicht mit Schlagwörtern gearbeitet werden soll/sollte, welche intelligenten Filter sollen/sollten verwendet werden?

Auf die Beantwortung zu Frage 17 wird verwiesen.

19. Inwieweit soll/sollte bei der Online-Durchsuchung vorher feststehen, dass sich der zu durchsuchende Datenträger in Deutschland befindet und damit der deutschen Rechtsordnung unterliegt?

    Wie soll/sollten die Erkenntnisse über den Standort des Datenträgers erlangt werden?

Die Durchführung einer Online-Durchsuchung würde nur nach intensiver Vorbereitung und Vorklärung erfolgen. Dadurch soll unter anderem sichergestellt werden, dass der Einsatz im Geltungsbereich des deutschen Rechts erfolgt. Im Übrigen wird auf die Beantwortung zu Frage 4 verwiesen.

20. Sollen/sollten Abkommen mit anderen Staaten getroffen werden, welche einen Eingriff in die Souveränität dieser Staaten bei der Online-Durchsuchung von in diesen Staaten befindlichen Datenträgern gestatten?

22. Sollen/Sollten die Staaten, in denen sich (wie es zur Verschleierung des Absenders durch mehrere zumeist in verschiedenen Staaten befindliche, jeweils mit einer neuen IP-Adresse im Internet auftretende Server gängige Methode ist) „zwischengeschaltete" PCs befinden, bei einer Ermittlung des Absenders – also dem Nachverfolgen von IP-Adressen zum Auffinden des ursprünglichen Absender-PCs über in fremden Staaten befindliche Datenträger – informiert werden, wenn ja, auf welchem Weg, wenn nein, warum (im Hinblick auf die Feststellung der auf in diesem Staat befindlichen Datenträgern gespeicherten IP-Adressen und den damit verbundenen Eingriff in die Souveränität dieses fremden Staats) nicht?

23. Wie soll/sollte hinsichtlich der heimlichen Online-Durchsuchungen gewährleistet sein, dass staatliches Handeln für den Bürger überprüfbar bleibt, und welche – wie durchsetzbare – Rechtsposition soll/sollte dem Bürger gegenüber der heimlichen Online-Durchsuchung eingeräumt werden?

Auf die Antwort zu Frage 12 wird verwiesen.

21. Wenn nein, wie soll/sollte dem Problem der Berührung fremder Staatssouveränität bei der Online-Durchsuchung von nicht körperlich in Deutschland befindlichen Datenträgern begegnet werden?

Antwort entfällt – siehe Antwort zu Frage 20.

24. Wie hoch schätzt die Bundesregierung den Bedarf an zusätzlichen personellen Ressourcen für die Auswertung des durch die Online-Durchsuchungen gewonnenen Datenmaterials ein, und wie soll/sollte dieser Bedarf gedeckt werden?

Auf die Beantwortung zu Frage 4 wird verwiesen. Die personellen Ressourcen für die Durchführung einer Online-Durchsuchung können derzeit noch nicht prognostiziert werden.

Über geheimhaltungsbedürftige Einzelheiten der Tätigkeit des Bundesnachrichtendienstes, des Bundesamtes für Verfassungsschutz und des Militärischen Abschirmdienstes können Auskünfte der Bundesregierung nur gegenüber den zuständigen parlamentarischen Kontrollgremien erfolgen.

25. Sieht die Bundesregierung die Gefahr von erheblichen Schäden, wenn Kriminelle die bewusste Sicherheitslücke in der Software bzw. den „Bundestrojaner" nutzen, um an Betriebsgeheimnisse von Unternehmen zu gelangen, um die digitale Steuerung beispielsweise von Produktionsanlagen, Video- und Schließanlagen oder Tresoren zu beeinflussen oder sich auf andere Art und Weise auf Kosten von Unternehmen zu bereichern, und wie beurteilt die Bundesregierung die Gefahr von Regressforderungen gegen die Bundesrepublik Deutschland aufgrund solcher Vorgänge?

26. Wie beurteilt die Bundesregierung diese Frage im Hinblick auf drohende Wirtschaftsspionage durch ausländische Geheimdienste?

Auf die Beantwortung zu Frage 4 wird verwiesen.

27. Wie bewertet die Bundesregierung insbesondere im Hinblick auf die vom Bundesverfassungsgericht entwickelten Grundsätze zum Schutz des Kernbereichs der privaten Lebensführung den mit jeder Online-Durchsuchung verbundenen Eingriff in die digitale Privatsphäre der Benutzer der an das Internet angeschlossenen Datenträger in Abwägung zu den Beweissicherungsinteressen?

29. Inwieweit sieht die Bundesregierung die Verhältnismäßigkeit im Sinne des Subsidiaritätsprinzips bei heimlichen Online-Durchsuchungen im Vergleich zu offenen Ermittlungsmaßnahmen und der Überwachung der Telekommunikation gewahrt?

30. Inwieweit erwägt/erwog die Bundesregierung mehrfach bei demselben Benutzer weitere und/oder denselben Datenträger zu durchsuchen, ohne diesen schon nach der ersten Durchsuchung zu unterrichten?

31. Welche Bedeutung misst die Bundesregierung in der Beurteilung der Eingriffsschwere dem Unterschied bei, dass bei einer akustischen Wohnraumüberwachung diese auf die Gespräche und damit die Kommunikation zwischen mehreren Menschen abzielt, während die heimliche Online-Durchsuchung nicht aktuelle Kommunikation, sondern vielmehr gespeicherte Daten wie beispielsweise auch persönliche Aufzeichnungen erfasst?

Auf die Antwort zu Frage 12 wird verwiesen.

28. Wie bewertet die Bundesregierung den mit der Online-Durchsuchung ggf. verbundenen Eingriff in die digitale Privatsphäre unbeteiligter Dritter bzw. die Gefahr des Eingriffs bei ggf. der ermittelnden Behörde unbekanntem Mitgewahrsam unbeteiligter Dritter an dem zu durchsuchenden Datenträger bzw. weiterer in einem Netzwerk angeschlossener PCs unbeteiligter Dritter?

Siehe vorstehende Frage 27.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333